**服务要求**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1.项目建设内容**  **一、网络安全设备维保服务**  服务内容：   |  |  |  |  |  | | --- | --- | --- | --- | --- | | 序号 | 设备名称 | 品牌 | 规格型号 | 服务明细 | | 1 | WEB应用防火墙 | 深信服 | AF-2000-H644 | 需提供原厂维保服务★ | | 2 | 服务器 | 浪潮 | NF5270M4 | 产品质保 | | 3 | 行为感知平台 | 深信服 | 行为感知系统 | 需提供原厂维保服务★ | | 4 | 云安全服务平台 | 深信服 | SDSEC-1000-B606 | 需提供原厂维保服务★ | | 深信服端点安全软件V3.0 | | BVT-1000-V300 | | LAS-1000-V300 | | CSSP-DAS-400 | | 5 | 安全态势感知平台 | 深信服 | SIP-1000-C402 | 需提供原厂维保服务★ | | STA-100-E642 | 需提供原厂维保服务★ | | 服务频次 | | 每月巡检服务，不少于12次/年 | | |   设备维保服务内容：  1．对服务范围内软硬件设备的维保，包括定期的巡检、日常维护、故障部件的更换，设备参数的调整，必要的维护等确保上述软硬件设备安全稳定运行。  2．服务商应提供定期的全面巡检，及时发现并排除系统故障，调整系统运行参数，保证系统运行在良好状态。及时响应采购单位的调试、优化及故障排除等服务要求，确保服务范围内软硬件设备无故障、稳定运行。  3．服务商应制定周期性的维护计划，根据设备部件的预防性维护要求，对需执行的维护操作予以实施，对预计寿命终了的部件预先予以更换。  4．在服务过程中应采取科学、合理的运维手段，确保服务质量。服务范围内硬件设备故障如无法排除，及时更换原厂配件（硬件），不收取任何费用。服务过程中，应编制详尽、规范的维护资料。  5．现场技能培训：供应商还将在系统维护过程及故障排查过程中进行现场技能培训，使采购人系统管理人员在自身的运行环境中得到锻炼，对采购人当前系统有更加深刻的认识，以提高日常管理能力及应对突发问题的技能。  **二、安全运维服务**  具体服务内容如下：   |  |  |  | | --- | --- | --- | | **序号** | **项目** | **详细内容** | | 1 | 风险评估服务  ≥200个资产) | 针对采购人指定≥200个资产进行评估，并在后续服务过程中根据识别的资产变化情况触发资产变更等相关服务流程，确保资产信息的准确性和全面性；针对指定的资产的全面梳理（梳理的信息包含支撑业务系统运转的操作系统、数据库、中间件、应用系统的版本，类型，IP地址；应用开放协议和端口；应用系统管理方式、资产的重要性以及网络拓扑），并将信息录入到安全运营平台中进行管理；当资产发生变更时，安全专家对变更信息进行确认与更新； | | 2 | 安全运营监控服务  ≥200个资产 | 一、服务概述  围绕资产、漏洞、威胁、事件四个要素，通过“人机共智”模式针对≥200个资产持续进行7\*24H监测保障工作，结合云端安全运营中心及安全专家建议进行必要的现场处置；构建持续、主动、闭环的安全运营体系，以保障我校网络安全“持续有效”运营。  二、服务内容  1.实时监测网络安全状态，对攻击事件(包括但不限于境外黑客攻击事件、高级黑客攻击事件、持续攻击事件)；  2.实时监测网络安全状态，对病毒事件(病毒类型包含不局限于勒索型、流行病毒、挖矿型、蠕虫型、外发DOS型、C&C访问型、文件感染型、木马型等。)及时进行分析与预警,自动化生成工单；  3.结合威胁情报进行流行威胁通告与排查，安排安全专家排查是否对我校资产造成威胁并通知用户，协助及时进行安全加固；  4.每月主动分析病毒类、攻击类、漏洞利用类、失陷类的安全事件提供主动分析与响应并提供针对性解决方案；  6.安全专家每月对安全组件上的安全策略进行统一管理工作，确保安全组件上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果；  7.通过攻击日志分析，发现持续性攻击，立即采取行动实时对抗；  8.实时针对异常流量、攻击日志和病毒日志分析进行事件分析与处置，经过海量数据脱敏、聚合来发现安全事件；  9.针对分析得到的勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，快速恢复业务，消除或减轻影响；  10.通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务，同时还原攻击路径，分析入侵事件原因，对业务进行安全加固、提供整改建议、防止再次入侵；  11.完成态势感知日报、周报、月报分析汇总；管理和维护项目涉及到的网络安全设备,包括WAF\安全态势感知\上网行为管理\出口防火墙等(包括但不限于设备安全策略升级\安全设备底层系统升级\安全设备日常及定期巡检\安全设备补丁升级等安全设备系统加固运维工作)。 | | 3 | 脆弱性(漏洞）管理 | 一、服务概述  进行专业的漏洞管理，识别系统安全漏洞，借助漏洞管理平台，可以有效地追踪资产漏洞生命周期，清楚地掌握资产的脆弱性状况，实现漏洞全生命周期的可视、可控和可管。识别漏洞后提出切实可行的漏洞修复指导，输出可行的漏洞处置方案，我校审核通过后，协助我校对漏洞进行验证处置工作，对已修复后的漏洞进行复测，帮助采购人将漏洞的影响降到可接受范围内；  具体服务内容：  1.提供客观的修复优先级指导，不能以脆弱性危害等级作为唯一的修复优先级排序依据。排序依据包含但不限于资产重要性、漏洞等级以及威胁情报（漏洞被利用的可能性）三个维度（提供具备相关能力举证材料）  2. 提供脆弱性验证服务，针对发现的脆弱性问题进行验证，验证脆弱性在已有的安全体系发生的风险及分析发生后可造成的危害。针对已经验证的脆弱性，自动生成工单，安全专家跟进修复状态，各个处理进度透明，方便采购人清晰了解当前脆弱性的处置状态，将脆弱性处理工作可视化（提供具备相关能力举证材料）  3. 针对存在的漏洞提供修复建议，能够提供精准、易懂、可落地的漏洞修复方案（提供具备相关能力举证材料）  4.针对服务平台生成的工单，招标方可按需催单，用户可在服务平台上采用邮件等方式提醒安全专家加快协助处置，督促投标方第一时间处理（提供具备相关能力举证材料）  5. 对发现的漏洞建立状态总览机制，自动化持续跟踪脆弱性情况，清晰直观地展示脆弱性的修复情况，遗留情况以及脆弱性对比情况，使得招标方可做到脆弱性的可视、可管、可控（提供具备相关能力举证材料） | | 4 | 安全日志分析与响应服务 | 一、服务概述  对安全日志、流量进行分析研判并对发现的威胁进行定位、响应，及时采取措施降低威胁可能造成的影响，并做闭环处置安全事件。  二、具体服务内容：  1.对感知平台进行平台运行状况检查、安全探针状态检查、序列号检查、规则库检查、安全分析引擎检查；（提供具备相关能力举证材料）  2.对日志进行内网脆弱性分析、尝试入侵行为分析、潜在威胁分析和通告；  3.深度威胁分析和研判，包括对漏洞利用攻击事件、Webshell上传事件、Web系统目录遍历攻击、SQL注入攻击、系统命令注入攻击、信息泄露攻击深度、口令暴力破解、Web明文传输、弱密码、勒索病毒事件、挖矿病毒事件、蠕虫病毒事件、僵尸网络攻击事件、SMB扫描事件、RDP暴破&SMB暴破事件等事件进行深度分析研判；（提供具备相关能力举证材料）  4.对内网脆弱性、入侵行为、潜伏威胁等安全问题进行威胁主动响应，如授权情况下调整相关设备策略，固化实际可行的病毒解决方案等。（提供具备相关能力举证材料） | | 5 | 应急响应服务  按需 | 一、服务概述  按照国家网络安全法、教育部、教育厅、学校发布的应急响应预案及处理流程，当发生黑客入侵、数据泄露、木马病毒等突发安全事件时，及时提供包括事件检测与分析、风险抑制、问题处置、快速恢复业务，及时止损，最大化降低安全事件带来的影响。包含但不限于WEB安全事件、恶意程序事件、意制造、传播恶意程序，或是因受到恶意程序的影响而导致的信息安全事件。  二、具体服务内容：  1.基于主动响应和被动响应流程，对业务的页面篡改、通报、断网、webshell、黑链等各类严重安全事件进行紧急响应和处置的解决方案。执行安全设备防护策略添加修改，完善安全防护策略。（提供具备相关能力举证材料）  2.依托于安全防护组件和检测响应组件，实现入侵检测、0Day检测、后门检测、篡改检测、勒索病毒、挖矿病毒等安全检测，支持紧急电话、邮件、Web管理端、微信公众号等多种响应渠道和方式，结合云端安全专家团队和线下安全专家，对安全事件进行入侵影响抑制、入侵威胁清除、入侵原因分析、加固建议指导等服务实施。  3.及时进行溯源分析排查，根据WEB安全事件、恶意程序事件、网络流量攻击、信息破坏事件等不同事件的定级和响应级别，提供专业的安全整改加固建议。  4.入侵影响抑制：通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务。  5.入侵威胁清除：排查攻击路径，恶意文件清除。  6.入侵原因分析：还原攻击路径，分析入侵事件原因。  7.加固建议指导：结合现有安全防御体系，指导用户进行安全加固、提供整改建议、防止再次入侵。  三、供应商服务要求:  提供7\*24应急响应服务。安全事件要求应急团队须在5分钟内，对信息安全事件做出响应，并严格按照采购人信息安全等级要求迅速到达现场并解决问题，追根朔源，查找攻击源。其中一类、二类业务系统须1小时内到达现场。三类业务系统须2个小时内到达现场。一般性故障2小时内到现场，4小时内处理解决，紧急故障2小时内处理解决。每次故障处理完毕3个工作日内提供详细的《应急响应报告》。 | | 6 | 应急演练服务  （一年不少于2次） | 根据要求定制可实施的“网络安全应急演练方案”，根据采购人现场实际环境设计并搭建应急演练演习环境，提前测试并验证演练环境涉及到设备的可用性及流畅性，协助采购人组织应急演练实施，结合采购人网络安全要求制定对应的应急演练预案，撰写应急演练总结报告，协助采购人完善专项网络安全应急处理流程。 | | 7 | 重保现场值守服务  不少于10天 | 一、服务概述：  按照采购人要求在重要敏感时期实施现场值守，及时处理相关安全事件。  二、具体服务内容：  1.根据事件级别进行不同级别的响应方式，包括电话、现场等；协调其他外部资源进行处理；根据需要部署相关监测设备，在敏感时期进行安全风险监测；编制应急响应情况报告，说明事件原因、处置措施等；  2.当发生外部黑客入侵、数据泄露、木马病毒等突发安全事件时，提供包括事件检测与分析、风险抑制、问题处置、协助业务恢复的服务，能够协助用户快速止损，最大化降低安全事件带来的影响;  3.每次重保前1周内，需针对≥200个资产进行1次信息系统弱密码抽样筛查、数据中心主机操作系统基线核查，协助我校进行弱密码、操作系统策略不合规处理；  4.每次重保前1周内，需针对重要信息系统及网站(指定的50个Web资产)进行1次~~进行~~安全评估扫描，协助采购人发现和处理系统及Web漏洞；云端安全运营中心和安全专家团队有效协同7\*24H持续性开展网络安全保障工作,服务通过云端系统7\*24H持续监测+人工核验相结合的方式持续开展安全监测。  三、供应商服务要求:  提供7\*24应急响应服务。  安全事件要求应急团队须在5分钟内，对信息安全事件做出响应，并严格按照采购人信息安全等级要求迅速到达现场并解决问题，追根朔源，查找攻击源。其中一类、二类业务系统须1小时内到达现场。三类业务系统须2个小时内到达现场。一般性故障2小时内到现场，4小时内处理解决，紧急故障2小时内处理解决。每次故障处理完毕3个工作日内提供详细的《应急响应报告》。 | | 8 | 渗透测试服务 | 每年对学校信息系统（不少于5个）进行模拟黑客攻击行为通过远程或本地方式对信息系统进行非破坏性的入侵测试，查找针对应用程序的各种漏洞，帮助学校理解应用系统当前的安全状况，发现在系统复杂结构中的最脆弱链路并针对安全隐患提出解决办法，切实保证信息系统安全；得到采购人授权后方可开始实施渗透工作。  渗透测试结束后提供《渗透测试报告》报告应该阐明招标方业务系统中存在的安全隐患以及专业的漏洞风险处置建议 | | 9 | 网络安全培训服务 | 1.通过全员安全意识的理论培训和案例分析以及关键行为上的最佳实践指导，让信息安全“人防”保障有效支撑业务高效稳定运行。培训内容包括普通员工的上网安全、邮件安全、通信安全等常见的安全意识内容。保证学校全体在职人员年度人均培训时间不少于4个学时且信息化管理和技术人员人均培训时间不少于8个学时。  2. 提供不少于5天的CISP课程培训（含教材），并提供CISP考试报名服务。 | | 10 | 高级威胁及未知威胁分析服务 | 根据采购人资产清单，采用不同手段对资产进行全面的高级/未知威胁分析，避免或降低高级威胁利用造成的影响，提供不限于人工智能、大数据、容器等技术的检测手段，且支持无特征检测技术，有效应对恶意代码及其变种（提供服务相关功能截图证明） | | 服务要求 | | ★提供7\*24应急响应服务。  对信息安全事件实时响应并解决问题，追根朔源，查找攻击源。其中一类、二类业务系统须1小时内到达现场。三类业务系统须2个小时内到达现场。一般性故障2小时内到现场，4小时内处理解决，紧急故障2小时内处理解决。每次故障处理完毕3个工作日内提供详细的《应急响应报告》。 | |
| **2.系统集成任务**  包含但不限于：按学校要求做好相关设备集成的技术支持。 |